2018-10-03

Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping

Tam, K::0000-0003-2840-5715

10.1080/23738871.2018.1513053
Journal of Cyber Policy
Informa UK Limited

Published as: Kimberly Tam & Kevin D. Jones (2018): Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping, Journal of Cyber Policy, DOI: 10.1080/23738871.2018.1513053

Kimberly Tam kimberly.tam@plymouth.ac.uk
Kevin D. Jones kevin.jones@plymouth.ac.uk

Maritime Cyber-Security Policy: The Scope and Impact of Evolving Technology on International Shipping

Kimberly Tam and Kevin D. Jones

ABSTRACT

As the global maritime industry becomes increasingly dependent on advancing technology, it is important for the world to be more aware of, and understand, the possible scope and impacts cyberattacks can have on international shipping. This article explores the maritime-cyber landscape for security flaws related to the area of maritime operations with an emphasis on the system technology involved, how their vulnerabilities enable attacks with cyber elements, and possible outcomes. As ships become more sophisticated and connected, in order to meet the demands of shipping 90 per cent of the world's goods, the cyber risks increase. This article aims to analyse compressively the unique nature of maritime cyber and cyber-physical threats to influence maritime cyber policies and improve global fleet security by suggesting adjustments and additions to current codes and policy to cover more comprehensively cyber and cyber-physical risks.

Keywords: maritime; policy; cybersecurity

Introduction

Due to the nature of maritime- based travel and environments, modern ship technology is significantly different from both typical computing systems and traditional maritime tools. To understand the unique scope and impact of cyberattacks on the shipping industry, this article analyses traditional cyberattacks in conjunction with knowledge of modern maritime technology to present a range of plausible maritime cyberattack scenarios. We conclude this examination of cyber vulnerabilities and outcomes, specific to the shipping industry, by suggesting improvements to maritime cyber policy and demonstrating their potential improvements. This is key for global security (i.e. economic, physical and social) as the maritime industry is roughly 20 years behind equivalent sectors in terms of cybersecurity (Belmont 2016).

The scenarios provided in this article illustrate a range of possible maritime cyberattacks, as a complete list is still being compiled due to insufficient data on global fleet equipment and practices. A number of maritime cyber incidents have also not been disclosed to the public or misclassified as machine or human error (Rothblum 2000).

However, the threat is real, as illustrated by recent pen-testing and known cyberattacks (AJOT 2017), (Maersk 2017). Since these incidents only highlight a narrow set of technical vulnerabilities and possible outcomes, this article seeks to widen the scope of understanding by exploring the evolution of maritime systems into the cyber domain, including emerging trends within autonomous or remotely controlled vessels, and the potential impacts. This in turn informs our policymaking decisions within the increasingly intertwined maritime and cybersecurity fields.

In the past, attacks like piracy were a common threat and so physical defences are well understood. In contrast, modern cyber and cyber-physical attacks aimed at ships are significantly less understood and, therefore, less preventable with current codes and practices. The stealth ability and long attack durations of newer cyberattacks increases the number of cyberthreats in general, including maritime cyberthreats (BIMCO 2016), (Allianz Global Corporate & Specialty 2016). Such maritime cyberattack impacts include (1) business disruption, (2) theft of information, finance and cargo, and (3) damage to reputation, goods and environment. As ships grow increasingly automated, perhaps even achieving full automation within five years (Bruxelles 2016), these threats must be better defined and policy shaped to prevent future incidences.

This article analyses cyber vulnerabilities of significant maritime technologies. Cyberattack scenarios are then constructed from these known vulnerabilities to demonstrate plausible exploits and outcomes. With a better understanding of the scope of problems and impacts, this article analyses the state of maritime-cyber policy today and proposes changes to improve global maritime cybersecurity.

Background

The maritime sector is a critical component of global trade infrastructure and transportation. Furthermore, the significant amount of shipping-based travel crossing national lines creates an interesting geopolitical dimension to maritime cybersecurity, due to separate nations and their policies (Germond 2015). These policies, and any future policies, are heavily influenced by a nation's economic goals, environment goals, and other considerations. Maritime transportation as a sector, therefore, poses a unique cyber security problem. Shipping also differs from other modes of transportation, such as airplanes, cars and trains, as they use significantly different systems, have different

trip durations (months versus hours), and cargo volume. Thus, just as risk analyses differ between airplanes and trains due to each sector's unique characteristics, it is equally important to explore maritime cyberthreats, risks and vulnerabilities from a maritime

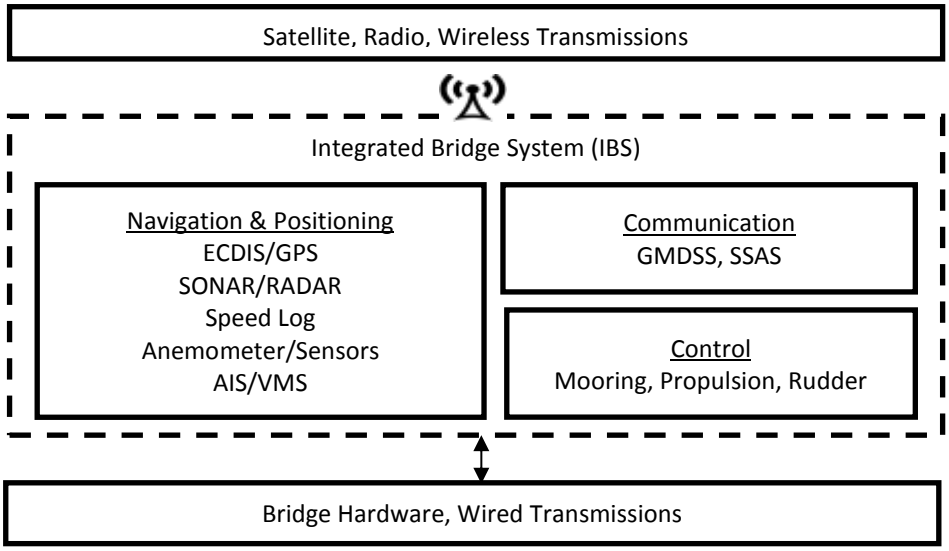

Figure 1. Overview of ship bridge systems.

perspective. That said, while different sectors make use of different systems (e.g. ECDIS, AIS) similarities in technology (e.g. radio-based) can be used to predict how the threats and threat outcomes will be different depending on the system or sector. For example, a similar vulnerability can exist in nuclear facilities and satellites, yet the exploitation of that vulnerability, and therefore the potential cyberthreat and outcome, are unlikely to be the same because of dissimilar system purposes (Unal and Lewis 2018).

However, one of the biggest differences between maritime cybersecurity and security in other sectors, is how comparatively poorly it is understood (Belmont 2016). This makes a comprehensive comparison of sector security difficult, but can be improved if maritime cyber incidences are better reported, as we hope the policy suggestions in this paper will enable. As shown below, these policies are aimed to mitigate cyber, and cyber-physical risks, which are different to the purely physical risks the maritime sector has primarily encountered so far. The range of a cyberattack increases the risks, as well as the increased anonymity of the attacker and the confusing prosecution laws for cybercrime. The assessment of risk, however, is not the goal of this

paper and for those interested in understanding the malicious players relating to maritime cyber and risk assessment, we refer to (BIMCO 2016) and (Tam and Jones 2018b).

From passenger ferries to large container ships sailing on international waters, the vast majority of all ships share at least two fundamental functions: navigation and propulsion, both of which are supported by a plethora of hardware and increasingly advanced software controls. Standard navigation systems like Global Positioning Systems (GPS), Automatic Identification Systems (AIS), and Electronic Chart Display and Information Systems (ECDIS) have increased physical safety through international regulation. However, with their technological advances come new cyberattack vectors to exploit and attack ships (Balduzzi 2014), (Coffeid 2014) and (AJOT 2017). A block diagram of several main ship-based systems can be found in Figure 1.

For historical reasons existing policies have primarily been designed for physical safety and efficient operations, not for addressing cyber or cyber-physical security. However, recent internationally standardised systems (several examples in Figure 1) increase the cyberattack surface of ships across the globe. As these systems are already known to have vulnerabilities, the arrival of remote-controlled and autonomous ships in the near future, is likely to intensify the effect of cyberattacks going forward.

Other industries, like rail (RSSB 2016), have developed cyberdefences to accommodate variances in their unique operations and environment, just as malware has been adapted to compromise systems in different industries. Given this, policies and technology defences developed for other industries would be based on assumptions inappropriate for shipping (e.g. banks are stationary and flights are less than 20 hours). This paper aims to understand the key dissimilarities of maritime cyber and, from that, shape effective security strategies. Several significant differences that set ships apart are their movement across international boundaries, the duration of their voyages (may be months), the average age of ships (20.3 years (International Chamber of Shipping 2016)), the mix of old and new systems, a nominally low bandwidth while at sea, and alternating between extreme isolation and global connectivity at international ports.

As previously mentioned, due to their mobility, ships are often difficult to secure using solutions or policies borrowed from other industries. Firstly, any physical or software-based security would have to be much more robust, as physical ship movement will expose its systems to a higher number of unknown networks, and across

international lines (e.g. geopolitics). Secondly, crew turnover and port interfacing make the physical and training aspects of cybersecurity especially challenging. Long voyages can also create large windows of opportunities for physical, cyber and cyber-physical attacks.

Unlike most onshore systems, ship builds and ship life cycles are much longer. Due to this, the certification of systems often support technology that are well-known but would be considered obsolete in other areas. Obsolete but certified hardware leads to the continued use of unsecure software. For example, Windows XP is not the most secure Windows operating system and organizations are highly encouraged to upgrade for security purposes. However, many ships cannot upgrade because of outdated hardware, which cannot easily be updated since there is a need to use devices that have been through appropriate certification standards for critical systems. As a result, the Royal and US Navies, have paid Microsoft to continue support for XP after Microsoft discontinued it (Goldman 2015). While upgrades have now been made, other ships are still vulnerable through legacy hardware, and the design cycle of newer ships are long enough that this problem will likely continue to exist.

The projected future of shipping, although driven by potential cost savings and better work environments for mariners, adds further intricacies as remote crews and autonomous ships will further complicate the maritime threat landscape and introduce a wider scope of possible attack outcomes and impacts (Bruxelles 2016) and (Shaikh 2017). By examining future and current technologies, the scenarios of the following section analyse what policy changes can increase cybersafety against a range of possible attacks and outcomes facing the evolving shipping industry. These primarily focus on ships, because even though port security is a major issue, it is better understood due its similarities with existing onshore infrastructure (IMO 2003). In comparison, securing a maritime vessel is significantly less understood and, as the potential weak link, must be addressed to secure global transportation infrastructure and for those who depend on it.

Maritime cyberthreat scenarios

This section describes several cyberattack scenarios based on known vulnerabilities in technology. While not real-world examples, the plausibility of these scenarios has been discussed with experienced mariners and extrapolated from known system vulnerabilities, rather than statistical data, as little exists. The interviews with and

survey responses from cybersecurity and maritime experts (contacted through existing contacts in both the security and maritime sectors) asked them to rank certain maritime system vulnerabilities within our scenarios as low, medium or high risks. For the ease of the reader, the referenced scenarios themselves can be found in Appendix A and are referenced by number within this section. This article discusses how known vulnerabilities have been exploited in technologically similar systems and demonstrates how events and system flaws can be exploited maliciously instead of triggered accidentally. With few past incidences to support the scenarios, supporting material to provide authenticity and plausibility are given. Scenarios also incorporate social factors as well as upcoming, near-future technology for a wider scope.

Although some of the resulting scenarios may seem a little extreme, they were designed to define the boundaries of plausible maritime cyberattacks and impact. They therefore illustrate various cyber-attacks, whether directly targeted by hackers, malicious software (i.e. malware) written by an attacker, or insider threats created by social engineering. Summaries, of scenario vulnerabilities and effects, cyber and cyber physical, can be found in Figures 2 and 4, which are organized based on a maritime cyber-risk assessment framework (Tam and Jones 2018b) and a breakdown of how these scenarios can be prevented with policy changes can be found in the following section.

Malware vulnerabilities

Malware can be easily installed physically by a variety of devices, including those not even capable of downloading content (e.g, an e-cigarette), via any port capable of reading data. In the first scenario, a USB port on the main integrated bridge system (IBS) computer is exploited. As a universal technology, the widely used USB is often the prime choice for physical malware infection (Maskiewicz, et al. 2014). In *Scenario 1*, a newly purchased USB drive held pre-installed malware, which was undetected. Today, introducing an infected device to the ship's bridge systems would be most easily achieved via social engineering, such as strategic product placement near or at shipping ports with low prices, which has been done previously to target similar systems using smartphones, as has been done in real life (Sulleyman 2017) and (Palmer 2017). Hence it is highly plausible that preinstalled, customized malware could corrupt maritime data (e.g. e-charts), and like the Stuxnet malware (Zetter 2014), the spread of malware via

USB could have little to no visible symptoms until the primary target is reached and attacked. Stuxnet is a state-level threat, likely performed by a state-level actor. Any vulnerability may be exploited, with the right level of resources, with a range of outcomes and severity depending on the vulnerability and the malicious actors (Tam and Jones 2018b) and (Shaikh 2017).

The specific malware type in *Scenario 1,* as seen in the Appendix section, is a command and control bot, many of which exist today, which can transmit stolen data back to the hacker and obey commands. Its moderate bandwidth activity may exceed ship capacity, slowing systems, but may go undetected without sufficient network analysis. Today, most cyberattacks are designed stealthily to prolong the exploit. However, in this scenario, the unintentional corruption of the charts had a noticeable impact and could have led to the malware's discovery if the right policies, checklists or training had been in place.

Scenario 1 and *Scenario 2* are a generalization of the cyber knowledge above applied to ships, current-day and near-future (Tam and Jones 2018a), and a few known incidents where maritime systems were compromised by malware from a USB device (Santamarta 2015) and via the internet (Sin 2013) in real life. With autonomy, the duration of unmanned voyages means more devices are updated at sea via the internet without human supervision or verification. Therefore, areas where shipboard policy and practice can be improved would be the prevention of infection with effective 'BYOD' and software update policy, as well as operation policy for mitigating the impacts of a successful attack with crew response training and computer-based intrusion and recovery solutions. Lastly, while malware infections aimed at significant systems (e.g. ECIS) could give an attacker more and quicker access, such an attack would be more difficult to achieve as the supply chain for important systems are likely to be more secure and closely monitored. Therefore an attacker may compromise a low-profile system first, like a USB device, meaning all systems must be protected for robust ship security.

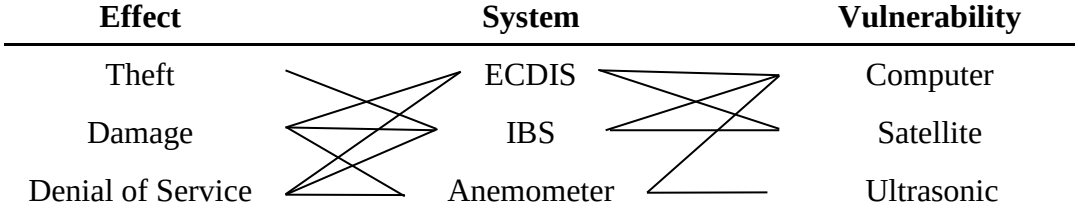

Figure 2. Malware scenario involving specific technological systems, known cyber vulnerabilities of those systems, and potential cyber/cyber-physical outcomes or effects.;

Jamming vulnerabilities

Signal jamming devices are relatively small and inexpensive to make or obtain, thus it would not be difficult to introduce a satellite or radio signal jammer to a ship heading to a dangerous hotspot like the Malacca Straits, a high flow area with high pirate activity. This is because, technologically speaking, it is easy to prevent signals from reaching their destinations by concentrating noise near the targeted receiver or emitter and cause signal congestion. Jamming is particularly effective on ships, as they are often very far from other signal sources, making those signals very weak and easy to jam theoretically and in practice (Coffeid 2014). A spectrum of frequencies, all of which can be jammed if the frequency range is known, can be found in Figure 3. General use examples of different frequencies with example maritime uses.

Use Examples	Maritime Navigation Signals	Navigation Aids	AM. Maritime Radio	Short wave radio	Broadcast TV, FM radio	Broadcast TV, Cell phone	Space and Satellite	Radio astronomy
Frequency	3kHz	30kHz	300kHz	3MHz	30MHz	300MHz	3GHz	30GHz 300GHz

Figure 3. General use examples of different frequencies and their jamming ranges.

In *Scenario 3*, the attackers were able to use social engineering to introduce a GPS and radio jammer to the ship. Social engineering may currently be the simplest way; however, attacks higher up the supply chain can also compromise a device or legitimate device update to introduce malicious hardware or software. Moreover, while social engineering may be hit and miss, popular ports with multiple targets would significantly increase the chances of a successful attack. Once introduced, jamming devices can be remotely controlled or given instructions (e.g. time or location) to activate at the most opportune moment. Even with a basic jammer onboard, cyberattacks can be extremely effective in disabling a ship as it may be unable to leave the jamming zone, update charts, or communicate effectively until the malicious device is disabled. While it can be very difficult to mitigate jamming threats with technology, operational policy could significantly prevent social engineering and detect unusual ship behaviour.

In *Scenario 4* of Appendix A, a shore-based attacker was able to use a jammer hidden in a large land-based vehicle. This lowers the attack's difficulty and risk of the attacker getting caught, but also lowers the number of available ship targets. Again, while it can be difficult to prevent these attacks with purely technological solutions, as jamming is a low-effort high-impact attack (Tam and Jones 2018b), changing policies and detailed checklists could greatly aid mariners in deterring, mitigating, and accurately reporting maritime cyberattacks like jamming. While there are reports of land-based jammers (Thomson 2013), the lack of robust reporting means there is no citable evidence for ocean-based instances, although there is anecdotal evidence of GPS jamming interfering with ships, particularly ferries transporting stolen cars. Today, several available automated mooring systems use radio-based remote controls to activate and deactivate the mooring system (MacGregor 2017). Generalizing from this, it is possible for an attacker to deploy similar land-based jamming for radio frequencies (see Figure 3). Furthermore, as auto-mooring systems are solely reliant on jammable wireless transmissions, and have no wired alternative, an attack could be highly effective.

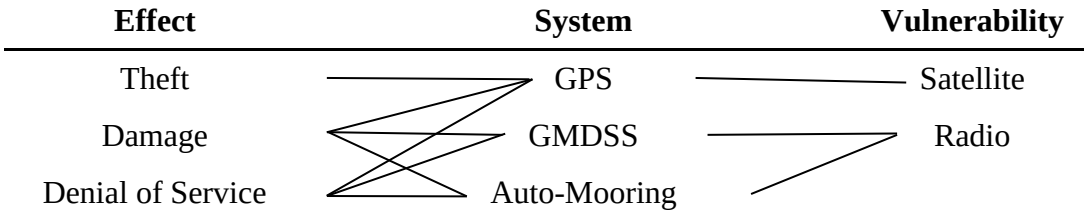

Figure 4. Jamming scenario involving specific technological systems, their known signal vulnerabilities, and potential cyber/cyber-physical outcomes/effects.

Denial of service (DoS) vulnerabilities

While some ships still carry analogue or hardwired systems (e.g., CAN, WAN, CANES and WSNs), as ships get larger, more advanced, and saturated with devices, many connect transmitters, repeaters, and sensors via network packet transmission. Generally speaking, today's ships are installing increasing numbers of sensors for monitoring cargo and ship functions to increase safety and efficiency (Yingjum, et al. 2010). In addition to that, future ships are more reliant on sensor data for computer-based decisions. This makes them particularly susceptible to denial of service (DoS) attacks

(Tam and Jones 2018a). While a physical DoS attack could be damaging sensors and/or transmitter hardware, *Scenario 5* explores a plausible cyber-physical attack that proposed policy development should help prevent if properly implemented. Specifically, in *Scenario 5*, a sensor network overload denies the bridge access to wireless rudder readings. Therefore, while the physical steering gear is operating normally, the bridge-mounted rudder angle indicator misleads the crew to thinking there is a physical rudder issue. If timed well, such an attack could have significant consequences. Many ships today lack secure network segregation or access control (BIMCO 2016) and malicious access to these networks can be achieved with compromised devices or crew members.

In *Scenario 5*, the compromised sensors flooded a non-segregated network with garbage data to slow legitimate packets, such as signals reporting rudder angles, from reaching the bridge on time. In cases where the network bandwidth can withstand the rogue sensor output, or the network is somewhat secure, a more sophisticated attacker may attempt other network-based attacks. For example, capturing and replaying packets could send contradictory signals to the bridge, which would be particularly effective in a UDP network, delaying or scrambling packets, and modifying packets. Additionally, altering an already connected device, attaching a new device, or gaining access to a network gateway may also be effective cyberattacks with a DoS impact. These network-based attacks are well known, and are still effective when used on well-protected systems, and would therefore be effective on ships as well (Hoque 2014).

In *Scenario 6*, a direct attack could also be made to the propulsion instead delaying network packets to the rudder angle indicator. Demand for new, economically friendly fuel has grown; however, incidences surrounding the storage and use of these fuels have also increased (Allianz Global Corporate & Specialty 2016). As sensors are required to measure and maintain fuel, and its data sent to the bridge or engineroom for analysis, network attacks can cause a myriad of exploits from a stall to an explosion by altering such data. As these systems evolve, it is essential that the technical vulnerabilities are mitigated or at least understood so that policy regarding cyberattack response can be made in conjunction. Also, as ships enter new environments (i.e. water tunnels), checklists, hygiene, and communication protocols must be set up to reduce the new associated risks. For both of these scenarios, as they map directly from denial of service to sensor networks and their vulnerabilities, no figure is given. However, if we

were to consider scenario variations, a mapping may be necessary to organize the possibilities.

Spoofing vulnerabilities

Spoofing (i.e. providing false data) is typically more sophisticated than jamming as it requires an understanding of the transmission protocols. However, the pay-off of spoofing instead of jamming is that the absence of a GPS signal often results in ship-wide alarms, whereas misdirection is less noticeable and can cause more subtle outcomes. In *Scenario 7*, saboteurs introduced a GPS spoofing device to the ship's environment. This was achieved by altering cargo manifests to define the malicious device as legitimate cargo to be loaded, similar to criminal smuggling activity in the past (Pasternack 2013). Generalizing from this incident, attackers could smuggle cargo containing spoofing devices onto vulnerable ships, specifically a cargo container in *Scenario 7*. Real attackers in this area have recently become much more technologically sophisticated, even using 3D printing to forge cargo seals after accessing shipping containers (CART 2017).

It is also likely that with the time it takes to manufacture a vessel, there is ample opportunity to try different approaches to sabotage the vessel for a desired impact. While such attacks require better planned and technologically advanced attacks in the current state of maritime security, the monetary incentive to do so would be higher. In the case of competing company sabotage, such attackers would also likely have the resources to develop and deploy high-level attacks (Tam and Jones 2018b) and be able to execute a direct attack or one further up the supply chain to compromise a ship build pre-launch. *Scenario 7* primarily demonstrates the possible outcomes from spoofing ship systems; however, a ship also relies on external shore-stored information and systems, which can also be spoofed to deploy a cyberattack without needing to compromise specific ships.

Generally speaking, virtual anti-collision beacons known as eAtoN beacons use traditional AIS technology to help navigate ships in locations where physical buoys cannot be used (reefs, ice routes, etc.) or low-visibility situations. There have been several studies on how to spoof and jam AIS broadcasts, and since there is no physical aspect to virtual AIS beacons, it makes it even harder to spot misleading information (Balduzzi 2014). This new adaptation of a well-established, maritime system (AIS) to a

more cyber-related system (eAtoN) is just one example of how maritime cyber encompasses an interesting blend of new, old, maritime, and traditional technology.

While the technology of eAtoNs can still be improved, as it is a relatively new application of AIS, policy can also be made to lessen the impact if this system is compromised. For example, if crew can accurately identify cyberattacks, protocols could enable fast communication ship-to-shore and ship-to-ship in order to quickly locate and fix these external vulnerabilities to prevent other potential incidences. Isolation of systems deemed non-trustworthy may also prevent cascading failures and remove untrustworthy information from crew decision-making. Extrapolating from these technologies and known vulnerabilities we present *Scenario 7* and *Scenario 8*.

Maritime cyber policy

As of 2018 the global implementation of robust maritime cybersecurity policy is essentially non-existent. One of the first analysis of the maritime cybersecurity state was in 2013 when the EU reported that, not only was there an international lack of maritime cybersecurity awareness, but existing policy catered to purely physical aspects of security and safety (ENSIA 2011). Despite some effort, it was not until recent attacks that there has been a real drive to design and put in place policy to counteract maritime cyber-attacks (Gallangher 2017). In this section we will discuss several phases of policy improvement that are proposed, based on the scenarios presented, that would significantly increase cybersecurity in the maritime community.

Firstly, it is the opinion of the authors that it would be sensible to start changes by adapting physical policies for cyber-physical security, as there already exist extensive efforts for physical maritime security. As this article has illustrated, it is likely that a significant portion of low-level attacks in the near-future will have a cyber-physical element, as opposed to entirely cyber-based. That said, it is likely that more sophisticated cyberattacks will arise as technology continues to evolve and be used. Secondly, this article discusses policymaking that can be used to prevent cyberattacks from occurring; and lastly, we discuss policies to assist crew, and other organizations tied to ship operations, in mitigating an occurring cyber-related incident or attack.

	Scenario							
Attack Category	1	2	3	4	5	6	7	8
Cyber		✓	✓	✓		✓	✓	✓
Cyber-Physical	✓				✓	✓		
Social Engineering	✓		✓		✓		✓	

Table 1. Primary attack categories per scenario.

Most of today's global maritime policies are produced by the International Maritime Organisation (IMO 2018), a specialized agency of the United Nations responsible for regulating shipping. The IMO has many partners, such as government departments for transportation, and subgroups for various aspects of shipping. Many international standards for maritime are defined by the IMO International Convention for the Safety of Life at Sea (SOLAS). This includes the International Ship and Port Facility Security (ISPS) Code, an amendment of SOLAS, which addresses some cybersecurity concerns. For example, the ISPS Code requires a ship security plan every five years. However, as discussed, the pace at which maritime technology evolves and becomes interconnected raises the question whether this would be effective and what changes will allow policies to be more flexible and effective as time passes.

Cyber-physical policy

As IMO policies provide smooth international shipping practices and prevent many physical accidents each year, and as these have been well tested and improved upon, relatively small additions to, or re-definitions of, existing policy could be a significant first step toward better maritime physical-cyber security. Adaptions to well-established codes for physical security could address the following cyber-physical risks. Despite varying malicious attackers, targeted systems, or outcome severity, we feel the following three categories are a sensible way to classify and address different cyber-physical threats:

- Physical attacks with a cyber element or outcome to improve success rate or mitigate risks of being caught;

- Cyberattack made possible with a physical action first;
- Cyberattack with a physical outcome such as a collision or cargo theft.

Attacks in the third category can be mitigated by policies suggested to address the first two categories, details below.

Physical attacks with a cyber element

The effects of cyberattacks or cyber-assisted attacks have already had an influence on policy, although sparsely in a few specific cases. Most significantly, with attackers abusing AIS to target ships (Balduzzi 2014), IMO policy has changed its strict mandatory policy to allow ship masters to turn off their AIS if it made them vulnerable, particularly in hotspots where piracy and armed robbery on ships are likely (IMO 2011). By improving technology, it may become possible to anonymize or secure identification information in these cases instead of disabling AIS; however, that may not be enough. That is why this article discusses possible changes to existing policy, particularly those designed for physical attacks, so that they also encompass similar attacks with cyber elements. This may include using intelligence collected from the internet, preventing communication (i.e. jam frequencies), and bypassing physical security (e.g. locks).

As an example, the UK Department for Transportation wrote guidance for the physical security related to piracy and other physical acts of violence against merchant shipping (Department for Transport 2011). This article uses the MGN 420(M) governmental policy of using armed guards to increase a ship's physical security but it can be adapted to incorporate cyber-physical attacks. For instance, it is recommended that guards and crew are aware of radio procedures and watch-keeping.

> Prior to entering areas where attacks have occurred, OOWs should practice and perfect all appropriate radio operational procedures and ensure all transmitters, including satellite ship earth stations are fully operational and available for immediate use on distress and safety frequencies (Department for Transport 2011).

However, in the case of a jamming attack, fully functional equipment may not be able to fulfil the communication needs of the crew, but existing policy can be modified to address such cyberattacks. Firstly, guards and crew can be trained to

recognize frequency-jamming attacks, and practices or checklists can determine a sequence of alternative communication channels to try until a connection is made. This would be effective as jamming techniques are unlikely to be able to jam the full spectrum constantly and can be bypassed once the attack is understood (Tam and Jones 2018b). Therefore, with a small adjustment to operations, ships can better counter such attacks. Secondly, policy and protocols can be modified so that prior to entering dangerous zones, a ship can send out periodical, covert, signals to onshore authorities. If that signal is cut off before the ship is known to be safe, it can be assumed that the ship is in distress, unable to communicate, and likely requires further action. These policies could help prevent or mitigate situations similar to the presented *Scenario 3* and *Scenario 4* (see Table 2).

Similarly, onboard crew or guards can be trained to prevent information leaks or social-based attacks, as they may provide attackers with useful information for a cyber-physical attack. For example, in one real world incident, because the crew of a ship were aware of an information leak, they were able to make course changes to mitigate the chances of an encounter in the Gulf of Eden, a known hot spot for such attacks (CyberKeel 2014). If this, or any other ship, were to have a physical encounter, it could then rely on physical safety such as locked doors to secure critical points and systems, such as the communication transceivers mentioned earlier. Therefore, any policy concerning these defences should also include cyberattack mitigation, such as PIN protection for doors and secure backup power to essential systems. We suggest the following suggestions to improve protections against physical attacks with a cyber element:

4.1.1.1: Crew training to recognize jamming attack;
4.1.1.2: Crew training to mitigate attacks with checklists and processes;
4.1.1.3: Enhancement of physical lockdown policy to include cyber lockdown.

Cyberattack made possible with a physical action

In general, the remote nature of ships can add a degree of cybersecurity. However, that security is severely reduced if a physical attack can overcome air-gaps and bypass local security. Typical cyber hygiene will deter the connection of most USB devices to ship systems (BIMCO 2016) but well-designed policy could add flexibility without

compromising security, as devices are often needed for software updates and broad rules may be ignored for convenience. If easily accessible and secure USB charging stations were provided, codes could state that all personal devices could only be charged at those locations. These isolated stations would protect systems with USB ports without inconveniencing crew. Firstly, this would add flexibility to the policy, as the number, types and dependency of USB-powered devices continue to grow (e.g. smartphones, cameras, e-cigarettes). Secondly, policy could dictate that USB meant for bridge or engineering need routine scans and checks, just as other systems do for physical safety, to reduce infection risks. Thirdly, policy could also assign specific uses for a set of USB drives to minimize attack vectors, a policy which may have helped prevent the attack in *Scenario 1*.

USB only represents one possible physical connection that can be used to make a cyberattack easier and, as existing physical-security policies are often significant aids in preventing unauthorized access to various access points on systems, it is likely that organizations can slightly alter current practices to ensure that critical access points to onboard computing systems and critical connections between systems are physically secured. This should decrease cyber-physical attacks by insider threats, saboteurs, and insecure interactions with other entities, such as port infrastructure and data networks. Furthermore, if implemented in conjunction with network security, this could significantly mitigate the attacks suggested in *Scenario 2*, *Scenario 5*, *Scenario 6* and *Scenario 7*, as both malicious physical and virtual access would be limited. Based on these potential attack scenarios for cyberattacks that are possible due to a physical action, we suggest the following policy changes. Table 2 also maps these policy suggestions to the Appendix A cyberattack scenarios that they may have been able to prevent or mitigate.

4.1.2.1: Allowed device connection policy;

4.1.2.2: Secure alternatives for charging and device network connections;

4.1.2.3: Separation of networks and devices with defined privilege regions.

Of the suggested policies, 4.1.2.1 – 4.1.2.3 resemble existing cyber policy the most and are similar to existing and in-draft cyber hygiene for ships (IET 2017) and (NOSAC 2016). However, the suggestions above can provide fine-grained instructions

which provide robust security without limiting mariners (e.g. approved USB charging stations) while effectively considering both cyber and physical cyberthreats.

Cyber policy for prevention

This section discusses directions maritime cyber practices can take in order to prevent cyberthreats from manifesting and to improve general maritime cyber defences. Some suggestions will build on the previous section of cyber-physical security, a proposed first step due to overlaps with traditional, well-established physical security. However, to consider future threats the following sections aim to prevent and mitigate maritime cyberattacks, particularly those concerning sophisticated and primarily cyber-based attacks. These will be more useful going forward, as maritime technology continues to evolve towards goals such as autonomy and remote control.

As alluded to in the previous sections, isolation can be used to secure different systems and networks from each other. This includes power and data networks. With the addition of physical security at critical access points, sensible policy for the interface of ship systems with other entities (e.g. USB, SCADA) makes it easier to continuously defend against, and prevent, maritime cyberattacks. This can build up from existing cyber-hygiene suggestions and adapt from existing policy for physical safety. For example, ships often have redundant navigation systems such as ECDIS (ECDIS info 2018) or SONAR. However, it is important from a cybersecurity perspective that identical systems do not share exact vulnerabilities, or else redundancy will only protect against accidents, not intentional cyberattacks. As seen in *Scenario 4*, a second auto-mooring trigger system like a hardwired trigger instead of relying solely on wireless transmissions could have mitigated the attack.

Unlike ship-based maritime security, port-based security has recently been more scrutinized and developed. For example, H.R.2878 Cybersecurity Information Sharing at Ports Bill and (IMO 2003) have policy for information security within ports. However, these often exclude detailed policy to prevent spreading cyber-risks ship-to-shore, vice versa, and ship-to-ship. Just as personnel and cargo are examined for physical threats like explosives (see below), it is equally important to create policies to screen electronics for malware and note the changes in risk and vulnerabilities during loading and unloading of hardware, software and data. Such policies may include traditional software checks, like signature-based analysis verifying the software

checksums to detect malicious additions, or the software version of trustworthy, well-tested, antivirus and firewall solutions.

> Prevent access to the port by **persons** without a legitimate reason to be there and prevent those persons with legitimate reasons to be in the port from gaining illegal access to ships or other restricted port areas for the purpose of committing unlawful acts (IMO 2003).

Crew and onshore management can also receive cyber-awareness training and be taught governance procedures concerning the maritime information and operational technology (IT/OT) of ship systems. This is particularly important for crew on semi-autonomous ships or those who will be using remote access to perform operations. As demonstrated in all the scenarios above, crew awareness could decrease the probability of a cyberattack. Furthermore, well-trained crew or hired guards can actively detect and mitigate an attack if it were to actually occur. This is especially important when considering more sophisticated attacks, such as the one in *Scenario 8*, as an attack may not be easily preventable and only present a small window for averting further incidents, if even detected. Suggested policy changes for cyberattack prevention are:

> 4.1.3.1: Appropriate cyber awareness training specific to ship installed systems;
> 4.1.3.2: Appropriate policy for interaction between ship and shore-based systems;
> 4.1.3.3: Clear lines of responsibility for individual IT and OT systems;
> 4.1.3.4: Established communication/alerts for cyber incidences and concerns.

Crew training IMO resolution A.1079 (28) must be adhered to in any suggested training programs under these policies. Moreover, the creation of any security-related alarm regarding ship control and safety must meet International Electrotechnical Commission (IEC) 61508 and 62443 standards, while onshore office-level management security alerts must operate under typical security policies under the International Organization for Standardization (ISO) 27000 series of documents. When considering existing standards, the categorization of cyber, cyber-physical, and system vulnerabilities in this article can be useful in structuring policy more effective and robust than past cyber-hygiene reports (NOSAC 2016) and (IET 2017).

Cyber policy for mitigation

Currently there exist policies for continuing operations despite system failure. However, during a cyberattack, a system that is not working properly is not necessarily broken (e.g., jammed communications in *Scenario 3*) and a working system is not necessarily providing trustworthy data (e.g., GPS spoof in *Scenario 7*). Therefore, policies and operation checklists should account for these possibilities, instead of only considering something as functioning or non-functioning. Understanding the difference is essential as cyberattacks can blur the line and cause both human and machine confusion. It is also important that policies mitigate the damage from compromised systems, such as system isolation or shutdown. Other courses of action may be to repair untrustworthy systems or proper reporting to local authorities, higher management and IT/OT departments.

Reporting is an interesting subject when concerning maritime cyberattacks. Currently there are dedicated channels and codes for communicating emergencies and incidents. However, it is unclear whether these practices should be used for cyberattacks, or if it would be better to introduce new codes and channels specifically to report cyber-related incidents and attacks, especially if the range of attacks and malware reach the levels seen in typical computing systems. It is possible that entirely new codes, and even communication technologies, will be essential in the future if the current options prove to be insufficient to support the cyber scenarios. Once maritime cyber incidences receive better reporting, faster effective responses can be made to reduce risks further.

Like prevention, the mitigation of cyberattacks in the maritime community must be adaptable to new attacks as they arise. This includes being adaptable to new technology solutions that prevent or mitigate jamming, spoofing, etc. More specifically, new policies will need to be derived to determine when and how new defences should be used, maintained, and protected. As mentioned, this is particularly important as remote control and autonomy both add complexity to onboard systems, increasing the attack surface, and remove or reduce the human element. Suggested additions for cyberattack migration can be found in Table 2 and the following bullet points.

4.1.4.1: Reporting mechanisms for ship-based cyber incidents;

4.1.4.2: Appropriate policy for patch and update for ship-based systems.

In conclusion, we present Tables 1 and 2 to demonstrate the wide scope and impacts of maritime cyber scenarios designed by the authors and how proposed policy can prevent or mitigate these attack scenarios if implemented.

Table 2. Suggested policy that would prevent cyber incidents in proposed scenarios

	Scenarios							
Policy	1	2	3	4	5	6	7	8
4.1.1.1: Jamming Training			✓	✓				
4.1.1.2: Robust Communication	✓		✓	✓				✓
4.1.1.3: Physical/Cyber Lockdown	✓	✓			✓	✓	✓	
4.1.2.1: Device Connections	✓				✓		✓	
4.1.2.2: Device Charging	✓				✓			
4.1.2.3: Network/Device Separation	✓	✓			✓	✓		
4.1.3.1: Cyber Awareness Training	✓	✓	✓	✓	✓	✓	✓	✓
4.1.3.2: Ship-Shore Interaction		✓	✓	✓		✓		✓
4.1.3.3: IT/OT Lines of Responsibility	✓				✓	✓	✓	✓
4.1.3.4: Cyber Reporting Alerts/Comms.	✓		✓		✓	✓		✓
4.1.4.1: Reporting Mechanisms	✓	✓	✓	✓	✓			✓
4.1.4.2: Patches and Updates	✓	✓			✓		✓	✓

Conclusion

In conclusion, maritime is clearly trailing other sectors in critical national infrastructure security and needs new approaches to regulation and training short term, and new systems long term. Unique factors in the shipping industry, particularly dynamic changes in maritime technology, economy, social, and environmental elements, present significant cybersecurity challenges to protect this critical international infrastructure. To address the global issue, the goal of this article was two-fold; first, to raise awareness and to provide insight on the possible scope and impacts of cyber vulnerabilities based on technology vulnerabilities, and second, to propose policy changes and additions to robustly improve maritime cybersecurity as a whole; from

cyber-physical to purely cybersecurity, today and for the near future. The authors presented several plausible attack scenarios extrapolated from existing technological vulnerabilities and shipping operations and applied the concepts to ships. Using this wide range of potential maritime cyber scenarios, we demonstrate how the proposed policy amendments could serve to prevent and mitigate the undesired cyberattack outcomes in each of the scenarios. We conclude that these policies can have significant, positive impact in real world situations in combating both known cyberthreats and some that have not yet occurred.

Appendix

Scenario 1: Malware on the bridge via USB

During a voyage, several devices are plugged into the primary computer on the bridge of a cruise ship and the USB port on the ECDIS system. In this scenario, the primary computer is separate from the ECDIS; however, they are often the same, which would have made this exploit even simpler. The devices connected include several USB drives, holding chart updates and miscellaneous documents, a few work smartphones and a digital camera for charging. Hours later, key bridge systems start to lag, and the ECDIS screen finally goes static. The crew decide to wait until they reach port to address the problem, as they have a second working ECDIS as per regulation (ECDIS info 2018). Unfortunately, although the main computer seems unresponsive, the malware continues executing silently, stealing and transferring sensitive data. After a while however, the hacker grows disinterested or has achieved their goal and commands the malware to wipe itself off the systems before the ship can be thoroughly examined.

Scenario 2: Software update attack on an autonomous ship

In this scenario, an autonomous oil-carrier is wholly reliant on satellite-based connections to receive necessary software updates during its long voyages. Securing the supply chain for the production, delivery, and use of all ship software is essential to maintaining trustworthy systems. However, as this ship is autonomous with no human verification, one of minor updates was compromised to introduce a virus to the ship's ultrasonic anemometer, a highly accurate wind measurer, and its wireless repeater. During the long voyage, the malware has the opportunity to spread to other systems if the underlying network lacks the right access permissions and security policies.

Scenario 3: Close proximity jamming aided with social engineering

A private yacht is about to sail through a zone known for pirate activity. It is suspected that this hotspot exists because it is close to a port that is a common rest stop for expensive yachts and the local government has few resources to deal with the levels of piracy activity. The yacht crew and passengers are alert and follow all safety protocols. However, at the edge of the known danger zone they lose GPS and both satellite- and radio-based communications like GMDSS. Alarms that GPS has been lost alerted the crew to the situation but they are unable to call for help. The officer of the watch suspects jammers are at work; however, the yacht is unable to sail out of range.

Scenario 4: Shore-based jamming to prevent or delay operations

A river ferry approaches its docking area during heavy peak commuter traffic. Every ship in this company's fleet had recently been upgraded with an automated mooring system to improve physical safety and operational efficiency, which has saved the company time and money so far. However, when the radio remote is used to trigger the automated mooring gear, it does not engage. The crew is able to dock the ferry manually without damage; however, a number of passengers are upset and delays permeated throughout the morning. This scenario can also be expanded to represent port and ship-based interactions, as humans are only one type of cargo, and as there have been cases of hacking ports to smuggle goods (Pasternack 2013). This is not an unreasonable extrapolation.

Scenario 5: Denial of sensor readings for critical operations

A large newly outfitted ship is sailing through a narrow traffic zone after a refitting stop to replace several damaged sensors. While navigating a strait with several streams of shipping lanes, the captain gives a command with a new heading. The helmsman attempts to follow the command, but the rudder angle reader is very slow to change, making it look like the rudder has becomes unresponsive or sluggish. In a moment of confusion during a critical manoeuvre, the probability of a collision is fairly high and even if a collision doesn't occur, a comprised system can cause other issues later on.

Scenario 6: Chokehold traffic jam

It is estimated that in 2023 the first shipping tunnel will be open for cruises and freight ships (The Guardian 2017). Based on previous incidences where power faults stopped trains in tunnels with significant outcomes (BBC 2014), we can postulate a scenario in which the attacker is able to stop a ship in the middle of the tunnel and stop all subsequent traffic. In this scenario we hypothesize that the most effective way to achieve this would be to deny access to fuel by maliciously denying physical access or by preventing access to important data on the engine status, likely causing an emergency shutdown to prevent any disastrous outcomes such as an explosion.

Scenario 7: GPS spoofing for small directional drift

Producing massive containers (e.g. Triple-E class) is becoming more common. In this scenario a well-known shipbuilder received a contract to deliver several new container ships. However, just prior to release, one ship has an incident with light damage when it went slightly off course and made contact with a shallow sandbank. Although the shipbuilding company quickly discovered and disclosed that the cyberattack was caused by a third-party device, one they quickly removed from the rest of their fleet, enough reputation damage had been dealt. As a result, other competing companies were able to improve their own position in the market.

Scenario 8: AIS misdirection by spoofing eAtoNs

A bulk carrier enters a foggy bay, guided by a series of virtual buoys. Because the local weather often creates low visibility, eAtoN have been attached to the location of bridge piles and other water level obstructions in the bay to lower the probability of collisions (Terdiman 2014). Despite AIS readings saying the ship had large margins from all obstacles, the ship trajectory seemed to pass very close to one of the bridge's piles. The trained crew realise that the AIS data was inaccurate and decide to slow down and navigate entirely by SONAR. However, they do not communicate to others what had just transpired.

References

AJOT. 2017. *Cyber Penetration Tests Underscore Maritime Industry's Nightmare Security.* https://www.ajot.com/news/channel/maritime.

Allianz Global Corporate & Specialty. 2016. "Safety and Shipping." *Annual Review*.

Balduzzi, M. 2014. *AIS Exposed Understanding Vulnerabilities & Attacks 2.0.* Black Hat.

BBC. 2014. *Eurotunnel Train Stopped in Channel Tunnel by Power Fault.* http://www.bbc.co.uk/news/uk-england-kent-28194074.

Belmont, K. 2016. *Maritime Cybersecurity: Cyber Cases in the Maritime Environment.* AAPA.

BIMCO. 2016. "The Guidelines on Cyber Security Onboard Ships Version 2.0." *International Chamber of Shipping, INTERTANKO, BIMCO and CLIA and ICS and INTERCARGO*.

Bruxelles, S. 2016. *Robotic Ship Leaves Humans in its Wake.* The Times. https://www.thetimes.co.uk/article/robotic-ship-leaves-humans-in-its-wake-hsqnsszg0.

CART. 2017. "Cargo and Road Transport Security Guide." https://www.sbrcentre.co.uk/media/2147/cart_security_guide_12mb.pdf.

Coffeid, J 2014. "The Threat of GPS Jamming." *Exelis*.

CyberKeel. 2014. *Maritime Cyber-risks.* NCC Group Publication.

Department for Transport. 2011. "Guidance to UK Flagged Shipping on Measures to Counter Piracy, Armed Robbery and Other Acts of Violence Against Merchant Shipping ."

ECDIS info. 2018. *ECDIS Regulations.* http://www.ecdis-info.com/ecdis_regulations.html.

ENSIA. 2011. *Cyber Security Aspects in the Maritime Sector.* https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1.

Gallangher, J. 2017. *Maritime Cyber Policy in Spotlight after Maersk Attack.* https://fairplay.ihs.com/safety-regulation/article/4288491/maritime-cyber-policy-in-spotlight-after-maersk-attack.

Germond, B. 2015. "The Geopolitical Dimension of Maritime Security." *Marine Policy*: 137-142.

Goldman, D. 2015. "Navy Pays Microsoft $9 million a Year for Windows XP." *CNN tech.* June. http://money.cnn.com/2015/06/26/technology/microsoft-windows-xp-navy-contract/index.html.

The Guardian. 2017. *Move over Suez, Hello Stad – Norway to Build World's First*

Hoque, N., M. Bhuyan, R. Baishya, D. Bhattacharyya, and J. Kalita. 2014. "Network Attacks: Taxonomy, Tools and Systems." *Journal of Network and Computer Applications* 40: 307-324. Elsevier.

IET. 2017. "Code of Practice Cyber Security for Ships." *Department for Transport.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf.

IMO 2003. *Code of Practice on Security in Ports.* MESSHP/2003/14.

IMO. 2011. *Piracy and Armed Robbery Against Ships in Waters Off the Coast of*

IMO 2018. *International Maritime Organization.* http://www.imo.org.

Somalia. MSC.1/Circ.1339.

International Chamber of Shipping. 2016. *Review of Maritime Transport.* United Nations Conference on Trade and Development (UNCTAD).

MacGregor. 2017. *Mooring and Auto-mooring Solutions.* https://issuu.com/cargotec/docs/mooring_and_auto-mooring_2017-low-r.

Maersk. 2017. *A. P. Moller Maersk Improves Underlying Profit and Grows Revenue in First Half of the Year.* August. https://edit.maersk.com/en/the-maersk-group/press-room/press-release-archive/2017/8/a-p-moller-maersk-interim-report-q2-2017.

Maskiewicz, J., B. Ellis, J. Mouradian, and H. Shacham. 2014. "Mouse Trap: Exploiting Firmware Updates in USB Peripherals." *8th USENIX conference on Offensive Technologies*.

NOSAC. 2016. "Cybersecurity/Cyber Risk Management On the U.S. Outer Continental." *National Offshore Safety Advisory Committee*. https://homeport.uscg.mil/Lists/Content/Attachments/579/Cyber%20Security%20Committee%20Final%20Report,%20rcvd%209%20May%202016.pdf.

Palmer, D. 2017. *IBM Warns of Malware on USB Drives Shipped to Customers*. https://www.zdnet.com/article/ibm-warns-of-malware-on-usb-drives-shipped-to-customers/.

Pasternack, A. 2013. *To Move Drugs, Traffickers are Hacking Shipping Containers.* https://motherboard.vice.com/en_us/article/bmjgk8/how-traffickers-hack-shipping-containers-to-move-drugs.

Rothblum, A. 2000. "Human Error and Marine Safety." *International Workshop on Human Factors in Offshore Operations.*

RSSB. 2016. *Rail Cyber Security.* Crown, Department of Transportation.

Santamarta, R. 2015. *Maritime Security: Hacking into a Voyage Data Recorder.* IOActive.

Shaikh, S. 2017. *Future of the Sea: Cyber Security.* Government Office for Science, Foresight.

Sin, B. 2013. *Offshore Oil Rigs Suffer from Malware Attacks.* https://www.slashgear.com/offshore-oil-rigs-suffer-from-malware-attacks-24271125/.

Sulleyman, A. 2017. *Android Malware.* https://www.independent.co.uk/life-style/gadgets-and-tech/news/android-malware-phones-infected-samsung-galalaxy-s7-nexus-5x-models-before-sale-a7626726.html.

Tam, K., and K. Jones. 2018a. "Cyber-Risk Assessment for Autonomous Ships." *C-MRiC Cyber Security* . IEEE.

Tam, K., and K. Jones. 2018b. "MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment." *Technical Report.* https://www.cscan.org/download/?id=1093.

Terdiman, D. 2014. *Virtual Buoys May Stop Ships from Crashing in Fog.* https://www.cnet.com/news/virtual-buoys-may-stop-ships-from-crashing-in-fog/.

Tunnel for Ships. https://www.theguardian.com/world/2017/apr/06/move-over-suez-hello-stad-norway-to-build-worlds-first-tunnel-for-ships.

Thomson, I. 2013. *Feds Arrest Rogue Trucker after GPS Jamming Disrupts Airport.* https://www.theregister.co.uk/2013/08/12/feds_arrest_rogue_trucker_after_gps_jamming_disrupts_newark_airport/.

Unal, B., and P. Lewis. 2018. *Cybersecurity of Nuclear Weapons Systems.* International Security Department, Chatham House.

Yingjum, Z., X. Shengwei, X. Peng, and W. Xinquan. 2010. "Shipping Containers of Dangerous Goods Condition Monitoring System Based on Wireless Sensor Network." *IEEE Networked Computing.*

Zetter, K. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown.